

# Irreducible polynomials with several prescribed coefficients

Junsoo Ha

January 27, 2016

## Abstract

We study the number of irreducible polynomials over  $\mathbf{F}_q$  with some coefficients prescribed. Using the technique developed by Bourgain, we show that there is an irreducible polynomial of degree  $n$  with  $r$  coefficients prescribed in any location when  $r \leq [(1/4 - \epsilon)n]$  for any  $\epsilon > 0$  and  $q$  is large; and when  $r \leq \delta n$  for some  $\delta > 0$  and for any  $q$ . The result improves earlier work of Pollack stating that a similar result holds for  $r \leq [(1 - \epsilon)\sqrt{n}]$ .

## 1 Introduction and Statement of Result

The problem of finding irreducible polynomials with certain properties has been studied by numerous authors. One of the interesting problems among them is the existence of an irreducible polynomial with certain coefficients being prescribed.

The early form of this problem is as follows. Let  $\mathbf{F}_q$  be the finite field of  $q$  elements and  $n$  be a given integer, and write a polynomial  $P = \sum_{k \leq n} x_k T^k$ . Then we ask if we can find an irreducible for any given pair of integers  $j, n$  and  $a \in \mathbf{F}_q$  satisfying  $x_j = a$ , except when  $a = 0$  and  $j = 0$ . This problem, widely known as the Hansen-Mullen conjecture, see [1], has been settled by Wan [2] when  $n \geq 36$  or  $q > 19$ ; the remaining cases were verified by Ham and Mullen [3].

One may ask if we can find an irreducible with several preassigned coefficients. In other words, we study the number of irreducible polynomials of degree  $n$  satisfying  $x_i = a_i$  for all  $i \in \mathcal{I}$ , when the index set  $\mathcal{I} \subset \{0, 1, \dots, n-1\}$  and a finite sequence  $a_i \in \mathbf{F}_q$  for  $i \in \mathcal{I}$  are given. Unless we assume that the location

of prescribed coefficients has certain properties, the best known uniform bound is due to Pollack [4], who proved that when  $n$  is large, there is an irreducible polynomial with  $\lfloor (1 - \epsilon)\sqrt{n} \rfloor$  prescribed coefficients.

The analogue of the Hansen-Mullen conjecture in number theory is to find rational primes with prescribed (binary) digits. Recently, Bourgain [5] showed that for some  $\delta > 0$  and for large  $n$ , there is a prime of  $n$  digits with  $\delta n$  digits prescribed without any restriction on their position. Thus it is believed that an analogous improvement holds for polynomials in finite fields.

In this paper, we show that we can prescribe a positive proportion of coefficients. The result presented here is the combination of several known ideas. The underlying setup in this type of problems is the circle method over  $\mathbf{F}_q[T]$ , which can be found in Hayes [6]. A recent application of this method, among others, can be found in Liu and Wooley [7] on Waring's problem. The work of Pollack [4] is also implicitly based on this method.

The main element of this paper is the combination of Pollack's estimate and the interpretation of the result of Bourgain [5] in finite fields, though it is greatly simplified thanks to the Weil bound, i.e., the analogue of the Riemann Hypothesis for irreducible polynomials.

Our main theorem is as follows.

**Theorem 1.1.** *Let  $\mathcal{I}$  be a nonempty subset of  $\{0, \dots, n-1\}$  and choose  $a_i \in \mathbf{F}_q$  for each  $i \in \mathcal{I}$ . We write as  $\mathcal{S}$  the set of monic degree  $n$  polynomials with  $T^i$  coefficient given by  $a_i$  for each  $i \in \mathcal{I}$ . Then if  $\rho := |\mathcal{I}|/n \leq 1/4$ ,*

$$\left( \sum_{\substack{P \in \mathcal{S} \\ P \text{ is irreducible}}} 1 \right) = \frac{\mathfrak{S} q^{n-|\mathcal{I}|}}{n} \left( 1 + O \left( \frac{\log_q \left( \frac{1}{\rho} \right) + 1}{q^{1/\rho - 4/(\rho+1)}} \right) \right) + O \left( q^{3n/4} \right), \quad (1)$$

where the implied constants are absolute, and

$$\mathfrak{S} = \begin{cases} 1 & 0 \notin \mathcal{I} \\ 1 + \frac{1}{q-1} & 0 \in \mathcal{I} \text{ and } a_0 \neq 0 \\ 0 & 0 \in \mathcal{I} \text{ and } a_0 = 0. \end{cases} \quad (2)$$

Then the following corollary is a direct consequence of this theorem.

**Corollary 1.2.** *We have the following.*

1. *There is  $\delta > 0$  so that for any  $q, n$ , there is an irreducible polynomial*

of degree  $n$  with  $[\delta n]$  prescribed coefficients, unless the constant term is prescribed to 0.

2. For any  $n \geq 8$ ,  $0 < \epsilon < 1/4$  and  $q \geq q_0(\epsilon)$  for some large  $q_0$ , there is an irreducible polynomial of degree  $n$  with  $[(1/4 - \epsilon)n]$  prescribed coefficients, unless the constant term is prescribed to 0.
3. When  $n$  is large and  $r = o(n)$ , the number of irreducibles of degree  $n$  with  $r$  prescribed coefficients is  $\mathfrak{S}q^{n-r}(1 + o(1))/n$ .

The implied constants can be explicitly computed and we conclude as follows.

**Theorem 1.3.** *Suppose  $n \geq 8$ ,  $q \geq 16$ , and  $r \leq n/4 - \log_q n - 1$ . Then there exists monic irreducible polynomial of degree  $n$  with  $r$  prescribed coefficients, except when 0 is assigned in the constant term. We conclude the same when  $q \geq 5$ ,  $n \geq 97$ , and  $r \leq n/5$ ; or when  $n \geq 52$ ,  $r \leq n/10$  for arbitrary  $q$ .*

## 1.1 Notation

From now on, let  $T$  be an indeterminate and we denote the ring of polynomials over  $\mathbf{F}_q$  by  $\mathbf{F}_q[T]$ . The polynomials play a parallel role of integers in this paper, so we keep the polynomials in  $\mathbf{F}_q[T]$  as lowercase Latin letters whereas parameters are usually written in capital letters. In particular, we substitute the variable  $n$  in Theorem 1.1 by  $X$ . Also, we use  $m$  for monic polynomials and  $\varpi$  for monic irreducible polynomials. The variable  $g$  usually means the modulus, and is assumed to be monic.

Following the setup of Hayes [6], we let  $\mathbf{K}_\infty$  be the formal power series  $\mathbf{F}_q((1/T)) = \{\sum_{i \ll \infty} a_i T^i\}$ , which is the completion of  $\mathbf{F}_q[T]$  in the usual norm

$$|m| = q^{\deg m}$$

for polynomial  $m$  (with convention  $|0| = 0$ .) We extend this norm to  $\mathbf{K}_\infty$  by

$$|x| = q^L$$

where  $L$  is the largest index so that  $x_L \neq 0$  (here and from now on, whenever  $x \in \mathbf{K}_\infty$ , the subscripted  $x_k$  denotes its  $T^k$ -coefficient.)

We define  $\mathbf{T}$  by  $\{x \in \mathbf{K}_\infty : |x| < 1\}$ , and fix an additive Haar measure,

normalized so that  $\int_{\mathbf{T}} dx = 1$ . Finally we take a nontrivial additive character

$$\mathbf{e}(x) = \exp\left(\frac{2\pi i}{p} \operatorname{tr}_{\mathbf{F}_q/\mathbf{F}_p}(x_{-1})\right),$$

where  $p$  is the characteristic of  $\mathbf{F}_q$ . Then  $\mathbf{e}(x)$  has similar property as  $t \mapsto \exp(2\pi i t)$  in number theory. For one thing, we have for a polynomial  $a \in \mathbf{F}_q[T]$ ,

$$\int_{\mathbf{T}} \mathbf{e}(ax) dx = \begin{cases} 1 & a = 0 \\ 0 & a \neq 0. \end{cases}$$

We also adopt a convenient notation from Liu and Wooley [7] that  $\hat{X} = q^X$  and  $\mathcal{L}(Z) = \max(\log_q Z, 0)$ . For instance,  $X = \mathcal{L}(\hat{X})$  for  $X \geq 1$ , and  $\mathcal{L}(|m|) = \deg m$ . This is useful as we can write  $|m| = \hat{X}$  in place of  $\deg m = X$ . We also use  $\pi_q(X)$  for the number of monic irreducible polynomials with degree  $X$ .

Now we define for  $\alpha \in \mathbf{T}$ ,

$$\mathcal{S}(\alpha) = \sum_{|\varpi|=\hat{X}} \mathbf{e}(\varpi\alpha)$$

and

$$\mathcal{S}_{\mathcal{I}}(\alpha) = \sum_{m \in \mathcal{I}} \mathbf{e}(m\alpha)$$

where  $\mathcal{I}$  is as defined in Theorem 1.1. Then the number of irreducible polynomials in  $\mathcal{I}$  is represented by the integral

$$N = \int_{\mathbf{T}} \mathcal{S}(\alpha) \overline{\mathcal{S}_{\mathcal{I}}(\alpha)} d\alpha. \quad (3)$$

We use  $C_i$  to denote positive constants, which may depend on many parameters but is always absolutely bounded. For instance, we allow  $C = q/(q-1)$ , which is a constant depending on  $q$  but is absolutely bounded by 2; however, we do not allow  $C = 2^q$  as it is not absolutely bounded. Due to their abundant appearance, we label

$$C_{(q^B)} = \frac{q^B}{q^B - 1} \quad (4)$$

for positive  $B$  for the remainder of this paper, which is absolutely bounded by  $1 + 1/(2^B - 1)$  if  $B$  is bounded below by some positive constant.

## 2 Preliminaries

The following lemmas are counterparts in  $\mathbf{F}_q[T]$  for well-known theorems in number theory.

**Lemma 2.1** (Rational Approximation). *For each  $\alpha \in \mathbf{T}$ , there exist unique  $a, g \in \mathbf{F}_q[T]$  so that  $g$  is monic,  $|a| < |g| \leq \hat{X}^{1/2}$  and*

$$\left| \alpha - \frac{a}{g} \right| < \frac{1}{|g| \hat{X}^{1/2}}.$$

*Proof.* See Lemma 3 of [4] □

We define a Farey arc

$$\mathcal{F}\left(\frac{a}{g}, \hat{R}\right) = \left\{ \alpha \in \mathbf{T} : \left| \alpha - \frac{a}{g} \right| < \frac{1}{\hat{R}} \right\}. \quad (5)$$

From Lemma 2.1, we decompose  $\mathbf{T}$  into Farey arcs

$$\mathbf{T} = \bigcup_{|a| < |g| \leq \hat{X}^{1/2}} \mathcal{F}\left(\frac{a}{g}, |g| \hat{X}^{1/2}\right).$$

The Farey arcs in the above decomposition are pairwise disjoint; to prove, if  $\alpha$  lies in two Farey arcs centered at distinct fractions  $a_1/g_1$  and  $a_2/g_2$ ,

$$\frac{1}{\hat{X}^{1/2} \min(|g_1|, |g_2|)} > \max\left(\left| \alpha - \frac{a_1}{g_1} \right|, \left| \alpha - \frac{a_2}{g_2} \right|\right) \geq \left| \frac{a_1}{g_1} - \frac{a_2}{g_2} \right| \geq \frac{1}{|g_1 g_2|} \quad (6)$$

by the ultrametric inequality, which contradicts  $|g_i| \leq \hat{X}^{1/2}$ .

We define the set of major arcs by

$$\mathfrak{M} := \bigcup_{|a| < |g| \leq \hat{X}^{1/2}} \mathcal{F}\left(\frac{a}{g}, \hat{X}\right)$$

and the minor arcs by

$$\mathfrak{m} := \mathbf{T} - \mathfrak{M} = \bigcup_{|a| < |g| \leq \hat{X}^{1/2}} \mathcal{F}\left(\frac{a}{g}, |g| \hat{X}^{1/2}\right) - \mathcal{F}\left(\frac{a}{g}, \hat{X}\right).$$

In Section 3, we use the fact that  $\mathcal{S}(\alpha)$  is small on minor arcs, and is well approximated on major arcs, and that the most contribution of the integral (3)

came from the major arcs.

**Lemma 2.2** (Prime Number Theorem). *We have*

$$\frac{\hat{X}}{\mathcal{L}(\hat{X})} - 2\frac{\hat{X}^{1/2}}{\mathcal{L}(\hat{X})} \leq \pi_q(X) \leq \frac{\hat{X}}{\mathcal{L}(\hat{X})}.$$

*Proof.* See Lemma 4 of [4].

Let  $\phi(m)$  be the number of reduced residue classes mod  $m$ , i.e.,

$$\phi(m) = |m| \prod_{\varpi|m} \left(1 - \frac{1}{|\varpi|}\right).$$

In number theory, Euler totient function  $\varphi(n)$  has a lower bound (see Theorem 2.9 of [8])

$$\varphi(n) \geq e^{-\gamma} \frac{n}{\log \log n} \left(1 + O\left(\frac{1}{\log \log n}\right)\right)$$

for  $n \geq 3$ . The similar estimate holds for  $\phi(m)$  as well.  $\square$

**Lemma 2.3.** *For  $\deg m \leq q$  and  $T \nmid m$ , we have*

$$\frac{|m|}{\phi(m)} < e.$$

*If  $\deg m > q$ , and  $T \nmid m$ , we have*

$$\frac{|m|}{\phi(m)} \leq e^\gamma (\mathcal{L}\mathcal{L}(|m|) + 1).$$

*Proof.* The proof below is analogous to Theorem 2.9 of [8]. We write  $P_A = \prod_{\varpi \neq T, |\varpi| \leq A} \varpi$  for a positive integer  $A$ , and we say  $m$  is product of irreducibles with smallest possible degrees if  $P_A|m$  and  $m|P_{A+1}$  for some  $A$ , and let  $\mathcal{R}$  be the set of polynomials  $m$  satisfying

$$\frac{|m|}{\phi(m)} \geq \frac{|m_1|}{\phi(m_1)} \tag{7}$$

for any  $m_1 \in \mathbf{F}_q[T]$  such that  $|m_1| < |m|$ .

We claim that  $\mathcal{R}$  contains only the polynomials that are products of irreducibles with smallest possible degrees. If  $m$  is a polynomial with  $k$  distinct prime factors, we take  $m_1$  to be a polynomial with  $k$  prime factors that is the product of irreducibles of smallest possible degrees. Then if  $m$  is not the product

of smallest possible degrees,  $|m| > |m_1|$  and

$$\frac{|m|}{\phi(m)} = \prod_{\varpi|m} \left(1 - \frac{1}{|\varpi|}\right)^{-1} < \prod_{i \leq k} \left(1 - \frac{1}{|\varpi_i|}\right)^{-1} = \frac{|m_1|}{\phi(m_1)}$$

where  $\varpi_i$  is the choice of  $k$  polynomials with smallest possible degrees. Therefore  $m \notin \mathcal{R}$  and an element of  $\mathcal{R}$  is necessarily the product of smallest possible degrees.

We now show that it suffices to prove the lemma for  $m \in \mathcal{R}$ . For simplicity let  $f$  be the right hand side of the inequality, i.e.,  $f(m) = e^\gamma (\mathcal{LL}(|m|) + 1)$  if  $\deg m > q$  and  $e$  if  $\deg m \leq q$ . Note that  $f$  is an increasing function of  $|m|$ , since  $2e^\gamma > e$ . Suppose that we proved the lemma for all polynomials in  $\mathcal{R}$ , and that the lemma is false. Then there is a counterexample and let  $m_0$  be the counterexample whose degree is smallest. From the assumption,  $m_0 \notin \mathcal{R}$ . Thus there is a polynomial  $m_1$  such that  $|m_1| < |m_0|$  and  $|m_1|/\phi(m_1) > |m_0|/\phi(m_0)$ . Then

$$\frac{|m_1|}{\phi(m_1)} > \frac{|m_0|}{\phi(m_0)} > f(m_0) \geq f(m_1)$$

and thus  $m_1$  is also a counterexample for the lemma, which contradicts the choice of  $m_0$ .

It remains to prove the lemma for  $m \in \mathcal{R}$ . Since each polynomial in  $\mathcal{R}$  is the product of irreducibles with smallest possible degrees, we prove the lemma in this case.

When  $m = P_1$ ,

$$\frac{m}{\phi(m)} = \prod_{\deg \varpi=1, \varpi \neq T} \left(1 - \frac{1}{|\varpi|}\right)^{-1} = \left(1 + \frac{1}{q-1}\right)^{q-1} < e,$$

and thus all  $|m_1| < |m|$  satisfies (7).

When  $m = P_A$  with  $A > 1$ ,

$$\frac{|m|}{\phi(m)} < e \prod_{1 < r \leq A} \left(1 + \frac{1}{q^r - 1}\right)^{\pi_q(r)}.$$

Since  $r\pi_q(r) \leq q^r - 1$ ,  $\pi_q(r) \log(1 + 1/(q^r - 1)) \leq 1/r$  and thus

$$\frac{|m|}{\phi(m)} < e^{\sum_{1 \leq r \leq A} 1/r}.$$

From Euler-Maclaurin formula, we have

$$\sum_{r \leq A} \frac{1}{r} \leq \log A + \gamma + \frac{1}{2A}$$

and that for  $0 < x < 3$ ,

$$e^x \leq 1 + x + \frac{x^2}{2(1 - x/3)}.$$

Combining these two estimate, we have

$$\frac{|m|}{\phi(m)} < e^{\sum_{1 \leq r \leq A} 1/r} < A + \frac{1}{2} + \frac{1}{8(A - 1/6)}.$$

Since

$$\deg P_A = (-1) + \sum_{r \leq A} k\pi_q(k) \geq \sum_{k|A} k\pi_q(k) = q^A - 1,$$

we have

$$A \leq \log_q(\deg P_A + 1) \leq \mathcal{LL}(|P_A|) + \frac{1}{q^A - 1}$$

and thus  $|m|/\phi(m) < e^\gamma (\mathcal{LL}(|m|) + 1)$ .

Finally, for  $m|P_A$  and  $P_{A-1}|m$ , we have

$$\frac{|m|}{\phi(m)} = \frac{|P_{A-1}|}{\phi(P_{A-1})} \left(1 + \frac{1}{q^A - 1}\right)^{\deg m - \deg P_{A-1}}.$$

Therefore we observe that  $\log_q(|m|/\phi(m))$  is linear in  $\deg m$ . To be precise, let  $g(D)$  be the piecewise linear continuous function defined on  $D \geq \deg P_1$  whose breakpoints are  $D = \deg P_A$  for  $A \geq 1$  and satisfies  $g(\deg P_A) = \log(|P_A|/\phi(P_A))$ . From construction, we have  $\log(|m|/\phi(m)) \leq g(\deg m)$ . Also, we have  $g(D) \leq \log(\log_q D + 1)$  on each breakpoint of  $g$  and since  $\log(\log_q D + 1)$  is convex, we have  $g(D) \leq \log(\log_q D + 1)$  for any  $D \geq P_1$ . Therefore we conclude that

$$\frac{|m|}{\phi(m)} \leq e^{g(\deg m)} \leq e^\gamma (\log_q \deg m + 1) = e^\gamma (\mathcal{LL}(|m|) + 1)$$

as desired. □



## 2.1 Analysis on $\mathcal{S}_{\mathcal{I}}$

The norm of  $\mathcal{S}_{\mathcal{I}}$  can be explicitly computed.

**Lemma 2.4.** *We have*

$$\int_{\mathbf{T}} |\mathcal{S}_{\mathcal{I}}(\alpha)| d\alpha = 1.$$

*Proof.* The set  $\mathcal{S}$  can be rewritten as

$$\mathcal{S} = \left\{ m : |m| = \hat{X}, m = T^X + \sum_{j \in \mathcal{I}} a_j T^j + \sum_{\substack{j \notin \mathcal{I} \\ j < X}} x_j T^j \text{ for some } x_j \in \mathbf{F}_q \right\},$$

so we have

$$\begin{aligned} \mathcal{S}_{\mathcal{I}}(\alpha) &= \mathbf{e}(\alpha T^X) \prod_{j \in \mathcal{I}} \mathbf{e}(a_j T^j \alpha) \prod_{j \notin \mathcal{I}} \sum_{x_j \in \mathbf{F}_q} \mathbf{e}(x_j T^j \alpha) \\ &= \begin{cases} q^{X-|\mathcal{I}|} \mathbf{e}(\alpha T^X) \prod_{j \in \mathcal{I}} \mathbf{e}(a_j T^j \alpha) & \alpha_{-j-1} = 0 \text{ for all } j \notin \mathcal{I} \\ 0 & \text{otherwise.} \end{cases} \quad (8) \end{aligned}$$

From the definition,  $|\mathcal{S}_{\mathcal{I}}(\alpha)|$  depends only on the first  $X$  coefficients of Laurent series expansion, and thus it is constant on the range  $|\alpha - a/T^X| < 1/\hat{X}$  for each polynomial  $a \in \mathbf{F}_q[T]$ . Therefore

$$\int_{\mathbf{T}} |\mathcal{S}_{\mathcal{I}}(\alpha)| d\alpha = \frac{1}{\hat{X}} \sum_{|a| < \hat{X}} \left| \mathcal{S}_{\mathcal{I}}\left(\frac{a}{T^X}\right) \right| = q^{-|\mathcal{I}|} \sum_{\substack{|a| < \hat{X} \\ a_{X-j} = 0 \forall j \notin \mathcal{I}}} 1 = 1$$

which proves the lemma.  $\square$

We need the following covering lemma to apply Bourgain's technique where he simply used  $\kappa = 2$  in the theorem below. We slightly improve the constant so that we may apply when the density  $|\mathcal{I}|/X$  is close to  $1/4$ .

**Lemma 2.5** (Covering Lemma). *Let  $x, y$  be integers with  $1 \leq y \leq x$  and  $I \subseteq [1, x]$  be a given set of integers. Then there exists a set of consecutive integers  $J$  of length  $y$  so that*

$$\frac{|I \cap J|}{|J|} \leq \kappa \rho$$

where  $\rho = |I|/x$  and  $\kappa \leq 2$  is given by

$$\kappa(x, y, \rho) = \begin{cases} \frac{2}{\rho+1} & 1 < x/y < 2 \\ \frac{2u}{(u+1)\rho+(u-1)} & u-1 < x/y < u \\ 1 & y|x. \end{cases}$$

*Proof.* If  $x$  is multiple of  $y$ , the result is trivial because  $[1, x]$  can be covered by nonoverlapping intervals of length  $y$ , and by the box principle, at least one subinterval, say  $J$  satisfies the density  $|I \cap J|/|J| \leq \rho$ ; so we assume otherwise. We write  $|I| = z$  and  $u = \lceil x/y \rceil \geq 2$ . Now, we cover  $[1, x]$  into  $u$  intervals of length  $y$ , say  $J_1, \dots, J_u$  where the smallest element of each  $J_i$  is  $[(i-1)x/u]$ . Then we set  $\kappa_0$  to satisfy

$$\kappa_0 \rho = \frac{1}{y} \max_I \min_{1 \leq i \leq u} \{|I \cap J_i|\}.$$

The exact formula for  $\kappa_0$  is a bit complicated as  $y, z$  vary, but we can find some upper bound, and any upper bound for  $\kappa_0$  would work for  $\kappa$  in our lemma.

If  $u = 2$ , as  $I$  varies, the minimum density  $\min_i |I \cap J_i|/y$  gets largest when the intersection of  $I$  and  $J_1 \cap J_2$  is as large as possible. Let  $\rho_y = (2y - x)/x$ , which is the density of the overlapping interval out of the total length. If  $\rho \leq \rho_y$ , we get the trivial bound

$$\kappa_0 \rho = \frac{|I|}{y} = \frac{2\rho}{\rho_y + 1}.$$

If  $\rho > \rho_y$ , the minimum density gets largest when we take  $I$  to fill the overlap and equally split the remaining to  $J_1 - J_2$  and  $J_2 - J_1$ ; then

$$\kappa_0 \rho = \left\lceil \frac{|I| + |J_1 \cap J_2|}{2} \right\rceil \leq \frac{\rho + \rho_y}{\rho_y + 1}.$$

Thus in either case,  $\kappa = 2/(\rho + 1)$  works.

If  $u \geq 3$ , the minimum density gets largest when the intersection of  $I$  and  $\bigcup (J_i \cap J_{i+1})$  is as large as possible; that is when  $|I|$  is small,  $I$  intersects each  $J_i \cap J_{i+1}$  and the two tails  $J_1 - J_2, J_u - J_{u-1}$  equally by  $|I|/(u+1)$ , and when  $|I|$  is large,  $I$  covers all overlapping intervals and distribute remaining so that  $I$  intersects each  $J_i$  by almost equal length. To compute, let  $\rho_y = (uy - x)/x$ . If

$$\rho \leq (u+1)\rho_y/(u-1),$$

$$\kappa_0\rho = \frac{2|I|/(u+1)}{y} = \frac{2\rho u}{(u+1)(\rho_y+1)} \leq \frac{2u}{(u-1)\rho+(u+1)}\rho$$

$$\text{If } \rho > (u+1)\rho_y/(u-1),$$

$$\begin{aligned} \kappa_0\rho &\leq \frac{\frac{1}{u} \left( |I| - \frac{u+1}{u-1} |\bigcup (J_i \cap J_{i+1})| \right) + \frac{2}{u-1} |\bigcup (J_i \cap J_{i+1})|}{y} \\ &= \frac{\rho + \rho_y}{\rho_y + 1} \leq \frac{2u}{(u-1)\rho+(u+1)}\rho \end{aligned}$$

which proves the lemma.  $\square$

The following lemma, whose analogue in number theory is found in Lemma 3 of Bourgain [5], is the key advantage of this paper.

**Lemma 2.6.** *Let  $Q$  be such that  $\hat{Q}^2 \leq \hat{X}$ . We have*

$$\sum_{\substack{|g| < \hat{Q} \\ (aT, g)=1}} \left| \mathcal{S}_{\mathcal{I}} \left( \frac{a}{g} \right) \right| \leq \hat{X} q^{-|\mathcal{I}|} \hat{Q}^{2C_1|\mathcal{I}|/X}$$

where  $C_1 = \kappa(X, 2Q, |\mathcal{I}|/X)$  and  $\kappa$  is as defined in Lemma 2.5.

*Proof.* Any two fractions are pairwise separated by the norm of size  $\hat{Q}^{-2}$  by ultrametric inequality (see (6)), and thus the arcs  $\mathcal{F}(a/g, \hat{X})$  are pairwise disjoint. On the other hand, each term of  $\mathcal{S}_{\mathcal{I}}$  is  $\mathbf{e}(m\alpha)$  with monic polynomial  $m$ ,  $\mathbf{e}(m\alpha)\mathbf{e}(-T^X\alpha)$  remains constant when  $\alpha$  varies in norm of size  $< 1/\hat{X}$  and thus  $|\mathcal{S}_{\mathcal{I}}|$  is constant on  $\mathcal{F}(\alpha, \hat{X})$  for each  $\alpha \in \mathbf{T}$ . Therefore

$$\hat{X}^{-1} \sum_{\substack{|a| < |g| < Q \\ (aT, g)=1}} \left| \mathcal{S}_{\mathcal{I}} \left( \frac{a}{g} \right) \right| = \sum_{a, g} \int_{\mathcal{F}(a/g, \hat{X})} |\mathcal{S}_{\mathcal{I}}(\alpha)| d\alpha \leq \int_{\mathbf{T}} |\mathcal{S}_{\mathcal{I}}(\alpha)| d\alpha = 1. \quad (9)$$

We write for any integer  $X_1 \leq X$ , an index set  $\mathcal{I}_1 \subseteq \{0, \dots, X_1 - 1\}$  and a finite sequence  $a_j \in \mathbf{F}_q$  for  $j \in \mathcal{I}_1$ ,

$$\mathcal{S}_{\mathcal{I}_1}^{(X_1)}(\alpha) = \sum_m \mathbf{e}(m\alpha)$$

where  $m$  runs over all monic polynomials of degree  $X_1$  whose  $T^j$ -coefficient is  $a_j$  for any  $j \in \mathcal{I}_1$ , to emphasize the dependency on  $X_1$ . As we can see in (8),

$\left| \mathcal{S}_{\mathcal{I}_1}^{(X_1)}(\alpha) \right|$  does not depend on the choice of  $a_j \in \mathbf{F}_q$  and since we only use it with the absolute value, we do not write  $a_j$  for simplicity. Following (9), we have for any integer  $Q$  and any index set  $\mathcal{I}_1 \subseteq \{0, \dots, 2Q-1\}$ ,

$$\frac{1}{\hat{Q}^2} \sum_{\substack{|a| < |g| < Q \\ (aT, g)=1}} \left| \mathcal{S}_{\mathcal{I}}^{(2Q)} \left( \frac{a}{g} \right) \right| \leq 1.$$

Now, we take a subset  $\mathcal{J}$  of  $\{0, \dots, X-1\}$  consisting of consecutive numbers so that the length of the interval is  $2Q$  and its intersection with  $\mathcal{I}$  is of size

$$|\mathcal{I} \cap \mathcal{J}| \leq C_1 \frac{|\mathcal{I}|}{X} (2Q).$$

for  $C_1 = \kappa(X, 2Q, |\mathcal{I}|/X)$  by Lemma 2.5. We write  $\mathcal{J} = \{j_*, \dots, j_* + 2Q - 1\}$  for some  $j_*$ .

We put  $\mathcal{I}' = (-j_*) + \mathcal{I} \cap \mathcal{J}$ . Then we relate  $\mathcal{S}_{\mathcal{I}}^{(X)}$  with  $\mathcal{S}_{\mathcal{I}'}^{(2Q)}$  by

$$\begin{aligned} \left| \mathcal{S}_{\mathcal{I}}^{(X)}(\alpha) \right| &= q^{X-|\mathcal{I}|} \cdot \mathbf{1} \{ \alpha_{-j-1} = 0 \text{ for all } 0 \leq j \leq X \text{ and } j \notin \mathcal{I} \} \\ &\leq q^{X-|\mathcal{I}|} \cdot \mathbf{1} \{ \alpha_{-j_*-j-1} = 0 \text{ for all } 0 \leq j \leq 2Q \text{ and } j \notin \mathcal{I}' \} \\ &= q^{X-2Q} q^{|\mathcal{I}'|-|\mathcal{I}|} \left| \mathcal{S}_{\mathcal{I}'}^{(2Q)}(T^{j_*} \alpha) \right|. \end{aligned}$$

Therefore we apply (9) on  $\mathcal{S}_{\mathcal{I}'}$  to conclude

$$\begin{aligned} \sum_{\substack{|g| < \hat{Q} \\ (aT, g)=1}} \left| \mathcal{S}_{\mathcal{I}}^{(X)} \left( \frac{a}{g} \right) \right| &\leq q^{X-2Q+|\mathcal{I}'|-|\mathcal{I}|} \sum_{\substack{|g| < \hat{Q} \\ (aT, g)=1}} \left| \mathcal{S}_{\mathcal{I}'}^{(2Q)} \left( \frac{T^{j_*} a}{g} \right) \right| \\ &= q^{X-2Q+|\mathcal{I}'|-|\mathcal{I}|} \sum_{a, g} \left| \mathcal{S}_{\mathcal{I}'}^{(2Q)} \left( \frac{a}{g} \right) \right| \\ &\leq q^{-|\mathcal{I}|} \hat{X} \hat{Q}^{2C_1 |\mathcal{I}|/X}. \end{aligned}$$

□

The next lemmas are similar to Lemma 6 and 7 of [4].

**Lemma 2.7.** *Let  $a, g \in \mathbf{F}_q[T]$  be two given polynomials with  $(a, g) = 1$ , and  $g_0$  be such that  $g = g_0 T^k$  with  $(g_0, T) = 1$ . If  $1 < |g_0| \leq q^{\lceil X/(|\mathcal{I}|+1) \rceil - 1}$*

$$\mathcal{S}_{\mathcal{I}} \left( \frac{a}{g} \right) = 0$$

*Proof.* Suppose  $\mathcal{S}_{\mathcal{I}}(a/g) \neq 0$ . Then in the Laurent series expansion of  $a/g$ , the  $T^{-j-1}$  coefficient vanishes for any  $j \notin \mathcal{I}$  and  $0 \leq j < X$  from (8). We write  $J = \lceil X/(|\mathcal{I}| + 1) \rceil$ . Then by the box principle, there is at least  $\lceil (X - |\mathcal{I}|)/(|\mathcal{I}| + 1) \rceil \geq J - 1$  consecutive indices where the Laurent series of  $a/g$  vanishes.

We now show that if the Laurent series of  $a/g$  has  $J - 1$  consecutive zeros and write  $g = g_0 T^k$  with  $(g_0, T) = 1$ , then  $|g_0| \geq \hat{J}$ , which will prove the lemma. If the Laurent series has  $J$  consecutive zeros, we shift the series by multiplying some power of  $T$  to have

$$\left| \left\{ \frac{T^r a}{g} \right\} \right| \leq \left| \frac{1}{T^J} \right| \leq \frac{1}{\hat{J}}.$$

for some integer  $r$ , where  $\{x\}$  denotes the fractional part of  $x$ . However unless  $g_0 = 1$ , the left hand side is at least  $|g_0|^{-1}$ . Therefore  $|g_0| \geq \hat{J}$  as desired.  $\square$

## 2.2 Analysis on $\mathcal{S}(\alpha)$

The analysis on  $\mathcal{S}(\alpha)$  is fairly standard. We cite the following estimate as in Lemma 5 of [4]. We cite the original result due to [6], which is slightly more precise.

**Lemma 2.8.** *Let  $a, g \in \mathbf{F}_q[T]$  be two polynomials with  $(a, g) = 1$  and  $\gamma \in \mathbf{T}$ , satisfying  $|a| < |g| < \hat{X}^{1/2}$  and  $|\gamma| < 1/|g| \hat{X}^{1/2}$ . We have*

$$\mathcal{S}\left(\frac{a}{g} + \gamma\right) = \frac{\mu(g)}{\phi(g)} \pi_q(X) \mathbf{e}(\gamma T^X) \mathbf{1}_{|\gamma| < 1/\hat{X}} + R$$

with

$$|R| \leq \sqrt{\phi(g) \max(1, |\gamma T^X|)} \hat{X}^{1/2} \leq \hat{X}^{3/4}.$$

*Proof.* See Lemma 5 of [4] and (5.14) in Theorem 5.3 of [6].  $\square$

## 3 Proof of Theorem 1.1

Let  $\mathfrak{M} = \bigcup \mathcal{F}(a/g, \hat{X})$  where the union is taken over fractions  $a/g$  with  $|g| \leq \hat{X}^{1/2}$ , and  $\mathfrak{m} = \mathbf{T} - \mathfrak{M}$ . Then from Lemma 2.8,  $\max_{\alpha \in \mathfrak{m}} |\mathcal{S}(\alpha)| \leq \hat{X}^{3/4}$ .

Recall that the number of irreducible polynomials with prescribed coefficients is given by the integral

$$N = \int_{\mathbf{T}} \mathcal{S}(\alpha) \overline{\mathcal{S}_{\mathcal{I}}(\alpha)} d\alpha.$$

Then we have

$$\left| N - \int_{\mathfrak{M}} \mathcal{S}(\alpha) \overline{\mathcal{S}_{\mathcal{I}}(\alpha)} d\alpha \right| \leq \max_{\alpha \in \mathfrak{M}} |\mathcal{S}(\alpha)| \int_{\mathbf{T}} |\mathcal{S}_{\mathcal{I}}(\alpha)| d\alpha \quad (10)$$

and the right hand side is bounded by  $\hat{X}^{3/4}$  using Lemma 2.8 and Lemma 2.4. We recall that all  $\varpi$  and  $m$  appearing in the sums  $\mathcal{S}_{\mathcal{I}}(\alpha)$  and  $\mathcal{S}(\alpha)$  are monic, and thus  $\mathbf{e}(m\gamma) = \mathbf{e}(\gamma T^X)$  for  $|\gamma| < 1/\hat{X}$ . Therefore we have for  $|\gamma| < 1/\hat{X}$

$$\mathcal{S}\left(\frac{a}{g} + \gamma\right) = \mathcal{S}\left(\frac{a}{g}\right) \mathbf{e}(\gamma T^X)$$

and similarly for  $\mathcal{S}_{\mathcal{I}}(a/g + \gamma)$ . Then the main term can be written as

$$\begin{aligned} \int_{\mathfrak{M}} \mathcal{S}(\alpha) \overline{\mathcal{S}_{\mathcal{I}}(\alpha)} d\alpha &= \sum_{a,g} \int_{|\gamma| < 1/\hat{X}} \mathcal{S}\left(\frac{a}{g} + \gamma\right) \overline{\mathcal{S}_{\mathcal{I}}\left(\frac{a}{g} + \gamma\right)} d\gamma \\ &= \frac{1}{\hat{X}} \sum_{a,g} \mathcal{S}\left(\frac{a}{g}\right) \overline{\mathcal{S}_{\mathcal{I}}\left(\frac{a}{g}\right)} \end{aligned} \quad (11)$$

where the sum is taken over distinct fractions with  $|g| \leq \hat{X}^{1/2}$ .

We expect the main term of the integral to be

$$M := \frac{1}{\hat{X}} \left( \mathcal{S}(0) \overline{\mathcal{S}_{\mathcal{I}}(0)} + \sum_{b \in \mathbf{F}_q^*} \mathcal{S}\left(\frac{b}{T}\right) \overline{\mathcal{S}_{\mathcal{I}}\left(\frac{b}{T}\right)} \right). \quad (12)$$

If  $0 \notin \mathcal{I}$ ,  $\mathcal{S}_{\mathcal{I}}(b/T) = 0$  and thus  $M = q^{-|\mathcal{I}|} \pi_q(X)$ . If  $0 \in \mathcal{I}$ , we have by Lemma 2.8,

$$\mathcal{S}\left(\frac{b}{T}\right) = \frac{\pi_q(X)}{\phi(T)} + O\left(\sqrt{\phi(T)} \hat{X}^{1/2}\right)$$

where the implied constant is bounded by 1, and  $\mathcal{S}_{\mathcal{I}}(b/T) = \mathbf{e}(a_0 b/T) \pi_q(X) q^{-|\mathcal{I}|}$ .

Then

$$\begin{aligned} M &= \frac{\pi_q(X)}{q^{|\mathcal{I}|}} \left( 1 + \frac{\mu(T)}{\phi(T)} \sum_{a \in \mathbf{F}_q^*} \overline{e\left(\frac{a_0 b}{T}\right)} \right) + O\left(\frac{\sqrt{q} \pi_q(X)}{q^{|\mathcal{I}|} \hat{X}^{1/2}}\right) \\ &= \begin{cases} O\left(q^{1/2-|\mathcal{I}|} \hat{X}^{1/2}\right) & a_0 = 0 \\ \left(1 + \frac{1}{q-1}\right) \frac{\pi_q(X)}{q^{|\mathcal{I}|}} + O\left(q^{1/2-|\mathcal{I}|} \hat{X}^{1/2}\right) & a_0 \neq 0, \end{cases} \end{aligned}$$

where the implied constants are bounded by 1. Thus we have

$$M = \mathfrak{S} \frac{\pi_q(X)}{q^{|\mathcal{I}|}} + O\left(q^{1/2-|\mathcal{I}|} \hat{X}^{1/2}\right)$$

where  $\mathfrak{S}$  is defined in (2). It is not hard to replace  $\pi_q(X)$  by  $\hat{X}/\mathcal{L}(\hat{X})$  with a small error by Lemma 2.2.

Now we consider the remaining terms. Let  $J = \left\lceil \frac{X}{|\mathcal{I}|+1} \right\rceil$ . The remaining terms are

$$\sum_{|g|>1} \frac{\mu(g)^2}{\phi(g)} \pi_q(x) \sum_{(a,g)=1} |\mathcal{S}_{\mathcal{I}}(a/g)|.$$

The terms with  $|g| > 1$  and  $(g, T) = 1$  contribute

$$\sum_{|g|>1} \frac{\mu(g)^2}{\phi(g)} \sum_{(a,g)=1} \left| \mathcal{S}_{\mathcal{I}}\left(\frac{a}{g}\right) \right| = \sum_{|g|\geq J} \frac{\mu(g)^2}{\phi(g)} \sum_{(a,g)=1} \left| \mathcal{S}_{\mathcal{I}}\left(\frac{a}{g}\right) \right|$$

because  $\mathcal{S}_{\mathcal{I}}(a/g) = 0$  for  $|g| < \hat{J}$  from Lemma 2.7. Now we assume  $|\mathcal{I}| \leq X/4$ , and use  $C_2 = 1 - 2C_1 |\mathcal{I}|/X$ ; when  $|\mathcal{I}| \leq X/4$ ,  $C_2 \leq 1/5$ .

We apply the estimate in Lemma 2.3, and group the fractions  $a/g$  according to the degree of  $g$ . Combined with Lemma 2.6, when  $J < q$ ,

$$\frac{1}{q^{X-|\mathcal{I}|}} \sum_{|g|\geq J} \frac{\mu^2(g)}{\phi(g)} \sum_a \left| \mathcal{S}_{\mathcal{I}}\left(\frac{a}{g}\right) \right| \leq e \sum_{n\geq J} \frac{1}{q^{C_2 n}} + e^\gamma \sum_{n\geq q} \frac{\log_q n}{q^{C_2 n}}.$$

We have, for any integer  $A \geq 1$ ,

$$\begin{aligned} \sum_{n\geq A} \frac{\log_q n}{q^{C_2 n}} &\leq \left( \log_q A + \frac{1}{A \log q} \right) \sum_{n\geq A} q^{-C_2 n} \\ &\leq \left( \log_q A + \frac{1}{A} \right) C_{(q^{C_2})} q^{-A}. \end{aligned} \tag{13}$$

Using this formula, we have

$$\sum_{n\geq J} \frac{\log_q n}{q^{C_2 n}} \leq \frac{C_3}{q^{C_2 J}}$$

where  $C_3 = C_{(q^{C_2})} (e + e^\gamma + e^\gamma/q \log q)$ .

If  $J \geq q$ , we use (13) to obtain

$$\begin{aligned} \frac{1}{q^{X-|\mathcal{I}|}} \sum_{|g| \geq \hat{J}} \frac{\mu^2(g)}{\phi(g)} \left| \mathcal{S}_{\mathcal{I}} \left( \frac{a}{g} \right) \right| &\leq e^\gamma C_{(q^{C_2})} \frac{\log_q J + 1 + 1/J \log q}{q^{C_2 J}} \\ &= \frac{C_4 \log_q J + C_5}{q^{C_2 J}}. \end{aligned}$$

Thus we have

$$\begin{aligned} \frac{1}{q^{X-|\mathcal{I}|}} \sum_{|g_0| \geq \hat{J}} \left( \frac{\mu^2(g_0)}{\phi(g_0)} + \frac{\mu^2(Tg_0)}{\phi(Tg_0)} \right) \sum_{(a,g)=1} |\mathcal{S}_{\mathcal{I}}(a/g)| \\ \leq \frac{C_6 \mathcal{L}(\hat{J}) + C_7}{\hat{J}^{C_2}} \end{aligned} \quad (14)$$

for some  $C_6$  and  $C_7$ .

Therefore, the integral is

$$N = M + R_1 = \mathfrak{S} \frac{\pi_q(X)}{q^{|\mathcal{I}|}} + R_1 + R_2$$

with

$$|R_1| \leq \frac{\pi_q(X)}{q^{|\mathcal{I}|}} \cdot \frac{C_6 \mathcal{L}(\hat{J}) + C_7}{q^{C_2 J}}$$

and  $|R_2| \leq \hat{X}^{3/4} + q^{1/2-|\mathcal{I}|} \hat{X}^{1/2}$ . These errors and the replacement of  $\pi_q(X)$  by  $\hat{X}/\mathcal{L}(\hat{X})$  are absorbed in  $O(\hat{X}^{3/4})$ , which proves Theorem 1.1.

## 4 Evaluation of Constants and Proof of Theorem 1.3

We continue from the previous section. Let  $B$  be a constant to be specified later. We need to show the integral (3) is positive when  $q^{-|\mathcal{I}|} \pi_q(X) \geq |R_1| + |R_2|$ . We assume that  $|\mathcal{I}| \leq X/4 - \log_q X - B$ . Then we have  $\hat{X}^{3/4} \leq \pi_q(X) X^{-|\mathcal{I}|} q^{-B}$ , so the sufficient condition is

$$1 > \frac{C_8}{q^{C_2/\rho}} + \frac{1}{q^B} + O \left( \frac{\sqrt{q} \hat{X}^{1/2}}{\pi_q(X)} \right).$$

where  $C_8 = C_{(q)} \max \{C_3, C_4 \log_q(1/\rho) + C_5\}$ . The big-O term is numerically tiny and we exclude this from computation. Computing other constants, one



can show for  $q \geq 16$  and  $B = 1$ ,  $C_8 \leq 8.552$  and the right hand size is  $\leq 0.994$ . when  $q \geq 5$ ,  $C_8 \leq 11.684$  and for  $|I| \leq X/5$ , and  $B = 2$ ,  $C_8 \leq 12.335$  and the right hand side is  $\leq 0.884$ . If  $|I| \leq X/10$  and  $B = 2$ ,  $C_8 \leq 42.342$  and the right hand side is  $\leq 0.764$ . The second case is when  $X \geq 97$  and the last case is when  $X \geq 52$ , which proves Theorem 1.3.

## Acknowledgement

This article was revised from earlier draft of the author. The author like to thank the anonymous reviewers for carefully reading the article and suggesting helpful advice.

## References

- [1] T. Hansen, G. L. Mullen, Primitive polynomials over finite fields, Math. Comp. 59 (200) (1992) 639–643, S47–S50. doi:10.2307/2153081.  
URL <http://dx.doi.org/10.2307/2153081>
- [2] D. Wan, Generators and irreducible polynomials over finite fields, Math. Comp. 66 (219) (1997) 1195–1212. doi:10.1090/S0025-5718-97-00835-1.  
URL <http://dx.doi.org/10.1090/S0025-5718-97-00835-1>
- [3] K. H. Ham, G. L. Mullen, Distribution of irreducible polynomials of small degrees over finite fields, Math. Comp. 67 (221) (1998) 337–341.  
doi:10.1090/S0025-5718-98-00904-1.  
URL <http://dx.doi.org/10.1090/S0025-5718-98-00904-1>
- [4] P. Pollack, Irreducible polynomials with several prescribed coefficients, Finite Fields Appl. 22 (2013) 70–78. doi:10.1016/j.ffa.2013.03.001.  
URL <http://dx.doi.org/10.1016/j.ffa.2013.03.001>
- [5] J. Bourgain, Prescribing the binary digits of primes, II, Israel J. Math. 206 (1) (2015) 165–182. doi:10.1007/s11856-014-1129-5.  
URL <http://dx.doi.org/10.1007/s11856-014-1129-5>
- [6] D. R. Hayes, The expression of a polynomial as a sum of three irreducibles, Acta Arith. 11 (1966) 461–488.

- [7] Y.-R. Liu, T. D. Wooley, Waring's problem in function fields, *J. Reine Angew. Math.* 638 (2010) 1–67. doi:10.1515/CRELLE.2010.001.  
URL <http://dx.doi.org/10.1515/CRELLE.2010.001>
- [8] H. L. Montgomery, R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Vol. 97 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2007.